UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/916,785	07/27/2001	Gadiel Seroussi	10010554-1	8810

7590 10/03/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80528-9599

EXAMINER	
WILLIAMS, JEFFERY L	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 10/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/916,785	SEROUSSI ET AL.	
	Examiner	Art Unit	
	Jeffery Williams	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 July 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *10-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *10-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the communication filed on 07/01/2005

All objections and rejections not set forth below have been withdrawn.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 10 – 13 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 10 recites the limitation "environmental compressor" in line 4. There is insufficient antecedent basis for this limitation in the claim. For the purposes of examination it will be presumed that the applicant means: “environmental sensor”.

Claim 11 recites the limitation “merges the compressed data streams output by the compressors” in lines 5 and 6. There is insufficient antecedent basis for this limitation in the claim. There is no prior mention of “the compressors”. Furthermore,

there is no prior mention of "the compressed data streams" that are output by "the compressors". For the purposes of examination it will be presumed that the applicant means: "merges compressed data streams output by the compressor and the additional compressor for each of the one or more additional environmental sensors".

Claim 12 recites the limitation "to the received data" in line 2. There is insufficient antecedent basis for this limitation in the claim. A random number generator that "receives data", as claimed in claim 10, does not adequately provide antecedent basis for "the received data" as claimed. For the purposes of examination it will be presumed that the applicant means: "to received data".

Claim 13 is rejected by virtue of its dependency.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 10 – 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Eastlake et al., "Randomness Recommendations for Security", RFC 1750 in

view of Saints et al., "Method and Apparatus for Generating Random Numbers From a Communication Signal", U.S. Patent 6,430,170.

Regarding claim 10, Eastlake et al. discloses:

an environmental sensor that generates digitally encoded sensor values (Eastlake et al., page 10, sect. 5);

a compressor that receives the digitally encoded sensor values generated by the environmental compressor and compresses the received digitally encoded sensor values to generate a compressed data stream (Eastlake et al., pages 10 - 14, sect. 5.2). Eastlake et al. discloses that longer input bit streams should be mapped to shorter input bit streams, thus generating "quality" random data. Such compression is the function of a "compressor".

a random number generator that receives data from the compressed data stream and outputs random numbers (Eastlake et al., page 14, sect. 6; page 19, sections 6.3. and 6.3.1). Eastlake et al. discloses a random number generator that mixes random data from a plurality of sources and outputs a random number. This provides an "unguessable" random number. Furthermore, Eastlake et al. discloses that such "unguessable" random numbers (strong random seeds) are further used to generate sequences of strong random numbers for input into a random number generator.

Eastlake et al. discloses recommended random number generation techniques, including the collecting of "quality" random numbers by gathering and de-skewing input bit streams. After obtaining such "random input from a large number of uncorrelated

sources" the gathered random numbers should then be mixed together to generate a better random number. Eastlake et al. discloses that the collection of random bit streams is not instantaneous, but rather, takes time (Eastlake et al., page 10, sect. 5.1) Eastlake et al., however, does not disclose a method of determining *when* enough random input has been gathered so as to generate a better random number. Specifically, Eastlake et al. does not disclose *a monitor that receives the compressed data stream and monitors the compressed data stream to determine whether or not sufficient data has been received in the compressed data stream to generate a next random number; and a blocking switch controlled by the monitor to block output of a next random number by the random number generator when sufficient data to generate the next random number has not been received in the compressed data stream to generate a next random number.*

Saints et al. similarly discloses the generation of random numbers via the gathering and mixing of a plurality of random inputs. Furthermore, Saints et al. discloses a method of determining when enough random input has been gathered so as to generate a random number. Saints et al. discloses a "pool" or storage of random input data. The method of Saints et al. discloses a "monitor" that extracts a random number from the mixing of random input data in the pool "as soon as the pool is filled". Furthermore, the method of Saints et al. discloses a "blocking switch" that prevents the pool from being "considered ready for use" for generating a random number until the pool is filled (Saints et al., col. 9, lines 30-59).

It would have been obvious to one of ordinary skill in the art to combine the method of Saints et al. (for providing a monitor to monitor the collection of random data and a blocking switch to prevent random number generation until sufficient random data has been collected) with the recommended methods of Eastlake et al. This would have been obvious because one of ordinary skill in the art would have been motivated to generate a "quality" random number by preventing ("blocking") a system from generating a random number if an insufficient amount time has passed for the gathering of random input data in order to generate such a "quality" number.

Regarding claim 11, the combination of Eastlake et al. and Saints et al. discloses:

one or more additional environmental sensors (Eastlake et al., pages 7-10; page 14, sect. 6). Eastlake discloses a plurality of usable environmental sensors and discloses a method of mixing together the random input gathered by such sensors.

an additional compressor for each of the one or more additional environmental sensors (Eastlake et al., pages 10 - 14, sect. 5.2; sect. 5.3.1; page 19, sect. 6.2). Eastlake discloses that each of the gathered random inputs should be compressed so as to generate "quality random data". An example is given of a gathered audio bit stream which is first compressed before it is deemed to be "quality random data".

and a merging component that merges the compressed data streams output by the compressors to produce a merged, compressed data stream that is output to the

monitor and random number generator (Eastlake et al., page 14, sect. 6; page 19, sections 6.3. and 6.3.1).

Regarding claim 12, the combination of Eastlake et al. and Saints et al. discloses:

wherein the random number generator applies a hash function to the received data to produce a random number for output by the random number generation device (Eastlake et al., page 19, sections 6.3. and 6.3.1).

Regarding claim 13, the combination of Eastlake et al. and Saints et al. discloses:

wherein each environmental sensor monitors an environmental parameter, the environmental parameter selected from among environmental parameters including: temperature; sound; motion; light intensity; and ambient electromagnetic radiation (Eastlake et al., page 8, section 4.2; page 10, section 5; page 14; section 5.3.1). The combination of Eastlake et al. and Saints et al. do not disclose that environmental parameters include light intensity. However, it is obvious that, amongst a multitude of environmental parameters, light intensity is an environmental parameter. Thus, it is obvious that light intensity is an environmental parameter included amongst environmental parameters.

Response to Arguments

Applicant's arguments with respect to claims 1 – 9 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Ellison, Carl, "Cryptographic Random Numbers", IEEE P1363 Appendix E, Draft version 1.0, 11 November 1995.

Callas, Jon, "Using and Creating Cryptographic-Quality Random Numbers", June 1996, http://web.archive.org/web/19970518180734/http://www.merrymeet.com/jon/jon@worldbenders.com, accessed on 9/26/2005.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jeffery Williams
Assistant Examiner
AU: 2137

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER